

intercept.¹⁷⁰ These provisions are plainly sufficient to satisfy the “association” requirement of CALEA.

Furthermore, the 100 millisecond synchronization information requested by DOJ and FBI is not “reasonably available” to carriers. Specifically, while the time stamp in CDC messages will be very accurate with respect to the time an event is detected at the IAP, delays that are inherent in the design of telecommunications networks make it impossible to guarantee that the time an event is detected at the IAP will be within 100 milliseconds of the time the event – which may occur at any location on the network – actually took place.¹⁷¹ Thus, the synchronization information requested by the DOJ/FBI Petition is not reasonably available on existing networks. In order to provide the capability requested by DOJ and FBI, telecommunications network equipment would need to be redesigned to include an extraordinarily accurate, real-time signaling system, at great cost and for no business purpose. CALEA does not impose any such requirement.

IV. CALEA Does Not Require Delivery of Information That Is Neither Call Content Nor Call-Identifying Information

Thus far, these comments have discussed aspects of the punch list that DOJ and FBI categorize as call content or call identifying information, or at least as features

¹⁷⁰ See J-STD-025 §§ 5.4 (CDC message descriptions), 6.4.10 (defining TimeStamp parameter).

¹⁷¹ A familiar example of this problem is the several second delay that the user of a wireless phone often experiences between pressing the “send” button and receiving a ring or other indication of call progress.

needed for efficient law enforcement.¹⁷² Remarkably, four of the capabilities requested by the DOJ/FBI Petition – automated delivery of three types of surveillance status information, and standardization of interface protocols – cannot be fit into any of these categories. Indeed, DOJ and FBI do not even try to fit them into these categories.

A. Surveillance Status Information

The only statutory basis that the DOJ/FBI Petition asserts for the automated delivery of surveillance status information is the requirement of Section 103(a) of CALEA that telecommunications carriers “shall ensure” that their equipment is capable of providing access to communications and call-identifying information.¹⁷³ That is, DOJ and FBI argue that the requirements of Section 103(a) give rise to second-order obligations to provide capabilities that are not specified in Section 103(a). This argument is pure bootstrapping, and the Commission should reject it.

TIA and its members take seriously the obligation to provide the capabilities specified in CALEA and to ensure that their equipment has the necessary wiretap capabilities. But the assistance capability requirements of CALEA have nothing to do with the pre-existing obligation of telecommunications carriers under Title III to cooperate with law enforcement, nor with carriers’ practice of allowing law enforcement an opportunity to verify that interception equipment is functioning properly. Nothing in that practice nor in

¹⁷² The DOJ/FBI Petition specifically addresses call content in section III.A.2.a, and specifically addresses call-identifying information in sections III.A.2.b and .c. The remaining capabilities, discussed in sections III.A.2.d and .e, plainly are not included in either of these categories.

¹⁷³ 47 U.S.C. § 1002(a); see DOJ/FBI Petition at 52.

CALEA itself requires carriers to modify their networks in order to deliver surveillance status information in an automated fashion.

1. Continuity Check

The DOJ/FBI Petition requests that the Commission require carriers to provide a “continuity tone” to ensure that call content channels between the carrier and law enforcement are operational.¹⁷⁴ As noted in the Petition, law enforcement agencies have traditionally provided such signals themselves, usually in the form of a “C-tone” on the intercepted line.¹⁷⁵

Even if there were a statutory basis for this request, which there is not, its implementation would require costly and otherwise unnecessary modifications to existing switches. In order to deliver a C-tone to law enforcement, a carrier would need the ability to generate C-tone for use on inter-office lines, or “trunks.” At present, however, switches use C-tone only within the local loop. That of course is where law enforcement used to conduct its taps and where it used to get C-tone. But to implement this provision for wiretaps at the central-office switch, many carriers would have to incur considerable expense to install dedicated C-tone generators at the trunk level. If any further demonstration is necessary, this example surely shows the danger of adopting the DOJ/FBI view that CALEA requires carriers to guarantee that law enforcement will always receive every piece of data that it received in the past. What's more, the DOJ/FBI request

¹⁷⁴ See DOJ/FBI Petition at 54.

¹⁷⁵ See id. at 53.

fails to satisfy the requirements of § 107(b) of CALEA that a proposed standard be cost effective and minimize the impact on ratepayers.

2. Surveillance Status Message

The DOJ/FBI Petition further requests the inclusion of a periodic “surveillance status message” to verify that an interception is in place and working properly.¹⁷⁶ Again, this provision would be unduly burdensome and costly to implement. In the wireless context, for example, it would be extremely difficult to verify electronically that every relevant mobile switch (and every other piece of network equipment containing intercept-related data) is operational and properly configured for the intercept. Under the existing wireless architecture, there is no infrastructure in place that permits the carrier to poll network equipment in this fashion. Moreover, the development and implementation of such a capacity would be costly and complex, and would serve no other operational purpose. Thus, even if this DOJ/FBI request had a statutory basis, it would also fail to satisfy the requirements of cost-effectiveness and minimization of impact on ratepayers.

3. Feature Status Message

The DOJ/FBI Petition requests automatic updates of changes in a subscriber's call features and services (such as the addition of call waiting or call forwarding), so that law enforcement may determine how many call content channels are necessary for the intercept.¹⁷⁷ The Petition and the Proposed Rule are ambiguous,

¹⁷⁶ See id. at 54-55.

¹⁷⁷ See id. at 56-57.

however, as to the timeframe within which a carrier would be required to provide this information. Section 64.1708(g) of the Proposed Rule states that the carrier shall report a change in call features or services “when a request is made” by the subscriber, suggesting that the message would be triggered at the time that the subscriber first requests a new feature (typically, by calling the carrier). The next sentence, however, states that the message will report “when a subscriber first gains or loses the ability to invoke, without delay, network-provided features that would affect the delivery to law enforcement of call content or call-identifying information” Along the same lines, the section later provides that the message “shall be triggered and delivered when the service provider assigns or removes” a specified feature.

As a result, it is not clear whether the DOJ/FBI Petition contemplates the delivery of a feature status message (1) at the time the subscriber requests the change; or (2) at the time the change is actually executed, i.e., at the time the service becomes available to the subscriber (which could be several days after the request). This distinction is critically important to the feasibility of the proposed requirement. If carriers were required to provide feature status messages at the time that the subscriber submits a request, carriers would have to reconfigure entire customer service databases and other operating software to provide automatic messaging to law enforcement – a capability that is not even remotely supported by the present design of these systems. In some cases, the carrier might have to create interconnections to contractors and other service providers who are responsible for processing customer profile information. These modifications would be complex, time-consuming and very expensive. The CDT Petition makes this point well:

A subject may change services by mail or with a call from a facility not under authorized surveillance. Requiring the carrier to send a message to law enforcement on the target's line whenever services are altered in response to a customer request would require companies to digitize customer information and make it available over the data channel. This would be a significant precedent – requiring carriers to generate a type of on-line customer service profile solely for the benefit of government surveillance. This information currently is provided by subpoena and can continue to be provided in that manner. There is no basis in CALEA for requiring telecommunications carriers to add this information to their signaling channels.¹⁷⁸

For the above reasons, the request would be totally unwarranted even if feature status information constituted call-identifying information, which it does not.

B. Standardized Interface Protocols

The final capability requested in the DOJ/FBI Petition is a limitation on the number of interface protocols for delivery of intercept information to law enforcement.¹⁷⁹ Again, DOJ and FBI specifically concede that standardization of interface protocols is not required by CALEA: “Section 103 does not obligate carriers to use any particular interface protocol, and the Department of Justice and the FBI are not asking the Commission to impose any such obligation by rule.”¹⁸⁰ DOJ made a similar admission in February 1998, when it removed this requirement from the punch list:

¹⁷⁸ CDT Petition at 14.

¹⁷⁹ See DOJ/FBI Petition at 57-58.

¹⁸⁰ Id. at 57.

DOJ has reviewed the 11 “punch list” capabilities in reference to CALEA, its legislative history, and the underlying electronic surveillance statutes. In addition, DOJ reviewed a memorandum evaluating the “punch list” under CALEA that was prepared by the Office of General Counsel (OGC) of the FBI. As a result of its review, DOJ is providing the following legal opinion: . . . With respect to capability number eight (Standardized Delivery Interface), although a single delivery interface is not mandated by CALEA, DOJ believes that a single, standard interface would be cost effective and of great benefit to both law enforcement and telecommunications carriers.¹⁸¹

Despite these unambiguous concessions that a single delivery interface is not mandated by CALEA, the DOJ/FBI Petition argues, without any legal support whatsoever, that “a relatively small number of standardized protocols” are somehow required. This argument must fail.

The DOJ/FBI Petition distorts the record by arguing that “law enforcement agencies could be faced with prohibitive practical and financial burdens in equipping themselves to deal with scores of different protocols.”¹⁸² As DOJ and FBI are aware, J-STD-025 provides detailed rules for the format of acceptable protocols,¹⁸³ including “forward compatibility” and “backward compatibility” rules that guarantee that old protocols will not become obsolete as new protocols are introduced.¹⁸⁴ With respect to the format of interface protocols, CALEA provides only that carriers must deliver call content and call-identifying information “in a format such that they may be transmitted by means of

¹⁸¹ Colgate Letter at 1-2, 3 (footnote omitted, emphasis added).

¹⁸² DOJ/FBI Petition at 58.

¹⁸³ See J-STD-025 §§ 6.1, 6.2, 6.5.

¹⁸⁴ See id. § 6.6.

equipment, facilities, or services procured by the government to a location other than the premises of the carrier”¹⁸⁵ The detailed protocol specifications in J-STD-025 far exceed this requirement.

Furthermore, most telecommunications carriers already use one of a relatively limited set of protocols, such as Transmission Control Protocol/Internet Protocol (“TCP/IP”) and X.25. Nevertheless, there is a very important reason that the telecommunications industry cannot commit to specific protocols, and that CALEA does not require them to do so – that is, things change. The rapid evolution of telecommunications equipment and technology also leads to changes in the protocols that are used in telecommunications networks. For example, the TCP/IP protocol that is used for Internet transmissions has become very widespread over a period of just a few years. Congress recognized this reality of change by providing that CALEA

does not authorize any law enforcement agency or officer . . . to require any specific design of equipment, facilities, services, features or system configurations to be adopted by any provider of a wire or electronic communications service.¹⁸⁶

The adoption of rules by the Commission specifying standardized interface protocols at the request of law enforcement would violate this provision, and would constrain the development of new and improved protocols for use in telecommunications carrier networks. For example, if the Commission were to adopt the DOJ/FBI proposal that there be only five permissible interface protocols, it is unclear what would happen as new

¹⁸⁵ 47 U.S.C. § 1002(a)(3).

¹⁸⁶ 47 U.S.C. § 1002(b)(1).

protocols inevitably appear and old ones become obsolete. Would industry be required to “kick out” one of the old protocols in order to use a new one? Would this require law enforcement approval? What would happen to carriers still using the old interface protocol?¹⁸⁷ Certainly, there would also be other issues, many of which cannot be anticipated now because the development of new communications protocols (like the protocols that will be used for the proposed “Internet 2”) is a dynamic, ongoing process.

J-STD-025 strikes a careful balance by permitting such innovation to continue – as specifically provided by Congress – while providing sufficiently detailed specifications for protocols to guarantee the effective exchange of intercept information between telecommunications carriers and law enforcement. The Commission should not upset this balance, and it is not permitted by CALEA to do so.

V. The Inclusion of Location Tracking Capabilities in J-STD-025 Does Not Render It Deficient

The CDT Petition argues that J-STD-025 is deficient because it requires cellular and personal communications services (“PCS”) carriers, pursuant to a valid Title III order, to provide location information to law enforcement at the beginning and end of any

¹⁸⁷ The FCC should recognize that the majority of the many tens of thousands of wireline and wireless switches in the network may never be “CALEA-compliant” in their life cycle. These legacy systems were “grandfathered” by Congress, and absent significant upgrade or replacement, may never be upgraded to CALEA compliance unless law enforcement prioritizes particular switches higher than others, and provides the funding for retrofit. Thus, in the real world, for many, many years, the industry and law enforcement will be doing interceptions with both CALEA-compliant and non-CALEA-compliant equipment.

cellular or PCS communication.¹⁸⁸ Specifically, J-STD-025 provides that law enforcement will receive location information “when the location information is reasonably available at the intercept access point] and delivery is authorized, to identify the location of an intercept subject’s mobile terminal.”¹⁸⁹

CDT argues that location information is not call-identifying information, as FBI Director Freeh stated during the Congressional debate on CALEA.¹⁹⁰ TIA agrees that it is unclear whether delivery of location information is required by CALEA. CALEA defines call-identifying information to include “dialing or signaling information that identifies the origin, direction, destination, or termination of [a] communication”¹⁹¹ While location information does aid in “identif[ying] the origin, direction, destination, or termination of [a] communication,” location information is not “dialing or signaling information.” Furthermore, the hearing statements of Director Freeh, while not conclusive of the meaning of the text of CALEA, are persuasive support for the argument that location information is not call-identifying information. On the other hand, the DOJ Office of Legal Counsel has issued an opinion filed in the Commission’s recently-concluded “Enhanced 911” (“E911”) rulemaking,

¹⁸⁸ See CDT Petition at 8-10.

¹⁸⁹ J-STD-025 §§ 5.4.1, 5.4.5, 5.4.7, 5.4.8 (emphasis added).

¹⁹⁰ See CDT Petition at 9 (citing Digital Testimony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103rd Cong. 6 (1994) (testimony of FBI Director Louis Freeh) (“[Call setup information] does not include any information which might disclose the general location of a mobile facility or service.”).

¹⁹¹ 47 U.S.C. § 1001(2).

concluding that provision of location information in the E911 context does not violate CALEA.¹⁹²

Despite this ambiguity, the inclusion of location tracking capabilities in J-STD-025 does not render the standard “deficient.” As explained above, the telecommunications industry, in exercising its primary authority to set CALEA “safe harbor” standards, has consulted extensively with law enforcement in order to obtain the views of law enforcement on CALEA requirements. In some areas presenting ambiguities under CALEA, particularly where capabilities requested by law enforcement were reasonably available to industry, it has been possible to reach compromise on the features to be included in CALEA compliance standards. In the case of location tracking, industry agreed to include in J-STD-025 the obligation to provide to law enforcement the location of an intercept subject, but only at the beginning and end of each mobile communication. Industry rejected more aggressive proposals by law enforcement that were clearly unsupported by CALEA.¹⁹³

Under such circumstances – i.e., where (1) a capability requested by law enforcement is at least arguably covered by Section 103(a) of CALEA, (2) the capability is reasonably available to telecommunications carriers, and (3) industry and law enforcement

¹⁹² See Memorandum for John C. Keeney, Acting Assistant Attorney General, Criminal Division, from Richard L. Shiffrin, Deputy Assistant Attorney General (Sept. 10, 1996).

¹⁹³ For example, at the CTIA/FBI “legal summits” in September and October 1996, industry rejected the requests of law enforcement for “idle mode” tracking (i.e., provision of location information even when a mobile subscriber is not making a call) and for location information at the time of handoffs between cell sites.

have agreed to a reasonable compromise incorporating only the reasonably available capabilities into a CALEA standard – TIA submits that there is no basis for the Commission to conclude that the standard is “deficient.”

VI. Separate Delivery of Packet Header Information in Packet-Switched Networks Is Not Required by CALEA

The CDT Petition also alleges that J-STD-025 is deficient because it permits delivery of an entire packet data stream in response to a pen register order.¹⁹⁴ The problem with this argument is that it fails to recognize the important differences between circuit-switched and packet-switched technology.

The CDT Petition recognizes that “[i]n a packet switching environment, communications are broken up into individual packets, each of which contains addressing information that gets the packets to their intended destination, where they are reassembled.”¹⁹⁵ That is, packet-switched communications involve the combination of call content and call-identifying information within packets. The content portion of the packet is separated from the call-identifying information in the packet “header” only at the origination and termination points of the packet-switched communication.

Separation of the header from packet content is almost always performed by entities not subject to the capability requirements of CALEA – i.e., information service

¹⁹⁴ See id. Petition at 10-12; see also J-STD-025 § 4.5.2.

¹⁹⁵ CDT Petition at 10.

providers (“ISPs”) and individual subscribers to information services.¹⁹⁶

Telecommunications carriers almost always carry only assembled packets, and have no reason to develop the technology (both software and hardware) that would be required to separate packet headers from packet content. Significantly, this would not be the same technology that ISPs use to separate packet headers from content. ISPs receive packets directed to them (or to one of their customers), and send packets with a specific destination. Telecommunications carriers generally carry broad streams of packets which may be from multiple sources, and are not differentiated by ultimate destination. Furthermore, many packet data protocols (such as the TCP/IP protocol used on the Internet) permit packets from a single communication to travel to their destination by multiple routes.

Because of these circumstances, the technology does not now exist to permit telecommunications carriers to provide separated packet headers as call-identifying information. The CDT Petition does not provide any factual basis for a conclusion to contrary. Thus, it is manifest that such call-identifying information is not “reasonably available” to carriers.¹⁹⁷ At a minimum, it is apparent that there is no adequate basis in the factual record before the Commission for it to conclude that such information is

¹⁹⁶ See 47 U.S.C. § 1002(a) (capability requirements apply to “telecommunications carrier[s]”), § 1001(8)(C)(i) (“telecommunications carrier” does not include information service providers), § 1002(b)(2) (capability requirements do not apply to information service providers).

¹⁹⁷ In addition, if the Commission were to impose a requirement of provision of such information, the same considerations would provide a strong basis for an argument that implementation of the capability is not “reasonably achievable” under Section 109(b) of CALEA, 47 U.S.C. § 1008(b).

“reasonably available.” Therefore, if the Commission is inclined to impose on carriers any requirement to provide separated packet header information, it should do so only in a separate rulemaking proceeding commenced to gather further information on implementation of CALEA with respect to packet-switched communications.

In addition, the premise of the CDT argument that J-STD-025 is deficient with respect to its treatment of packet data is that the standard permits packet content to be delivered pursuant to a pen register order. However, it is unclear whether the courts will conclude that packet-switched communications can be accessed under a pen register order. As discussed earlier, substantive information cannot be delivered pursuant to a pen register order. For example, in Brown v. Waddell, discussed above, the Fourth Circuit rejected arguments that numeric messages sent to a display pager could be accessed under a pen register order.¹⁹⁸

By permitting packet content to be disclosed pursuant to pen register orders, J-STD-025 does not seek to prejudge whether courts in fact will be willing to issue such orders. It is as yet unresolved whether packet-switched communications should be considered as “substantive information” under the standard set forth in Brown v. Waddell. If the courts hold that packet-switched communications are substantive information under this standard, the privacy argument advanced by CDT will be moot, since law enforcement will not be able to access such communications under a pen register order in any event. However, since it is at least possible that the courts will consider packet-switched

¹⁹⁸ See Brown v. Waddell, 50 F.3d at 285.

communications to be available under a pen register order, J-STD-025 has been designed to make it possible to respond to such orders in a practical fashion.

VII. Conclusion

For the reasons set out above, the Commission should conclude that J-STD-025 is not "deficient," should deny the DOJ/FBI Petition and the CDT Petition, and should recognize J-STD-025 as a valid industry standard that is consistent with CALEA. In the alternative, if the Commission concludes that J-STD-025 is "deficient" in any respect, it should not adopt specific CALEA compliance standards, but should indicate the areas of deficiency and return to TIA the task of setting such standards. The Commission should also provide the reasonable transition time specified in CALEA for transition to any new FCC-mandated standard.

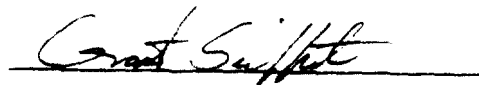
Respectfully submitted,



Stewart A. Baker
Thomas M. Barba
Maury D. Shenk
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 429-3000

**Counsel for Telecommunications
Industry Association**

May 20, 1998



Telecommunications Industry Association

Grant Seiffert
Director of Government Relations
Matthew J. Flanigan
President
1201 Pennsylvania Avenue, N.W.
Suite 315
Washington, DC 20004
(202) 383-1483

CERTIFICATE OF SERVICE

I, Maury Shenk, an attorney in the law firm of Steptoe & Johnson, L.L.P., hereby certify that I have on this May 20, 1998 caused to be served by first class mail, postage prepaid, or by hand delivery, a copy of the foregoing Comments of the Telecommunications Industry Association to the following:

The Honorable William E. Kennard
Federal Communications Commission
1919 M Street, N.W. - Room 814
Washington, D.C. 20554

The Honorable Harold Furchtgott-Roth
Federal Communications Commission
1919 M Street, N.W. - Room 802
Washington, D.C. 20554

The Honorable Susan Ness
Federal Communications Commission
1919 M Street, N.W. - Room 832
Washington, D.C. 20554

The Honorable Michael Powell
Federal Communications Commission
1919 M Street, N.W. - Room 844
Washington, D.C. 20554

The Honorable Gloria Tristani
Federal Communications Commission
1919 M Street, N.W. - Room 826
Washington, D.C. 20554

Christopher J. Wright
General Counsel
Federal Communications Commission
1919 M Street, N.W. - Room 614
Washington, D.C. 20554

Linda Morrison
Office of the General Counsel
Federal Communications Commission
1919 M Street, N.W. - Room 614
Washington, D.C. 20554

Daniel Phythyon, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W. - Room 5002
Washington, D.C. 20554

David Wye
Telecommunications Policy Analyst
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W. - Room 5002
Washington, D.C. 20554

Tim Maguire
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W. - Room 5002
Washington, D.C. 20554

A. Richard Metzger, Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W. - Room 500B
Washington, D.C. 20554

Geraldine Matisse
Chief, Network Services Division
Common Carrier Bureau
2000 M Street, N.W. - Room 235
Washington, D.C. 20554

Kent Nilsson
Deputy Division Chief
Network Services Division
Common Carrier Bureau
2000 M Street, N.W. - Room 235
Washington, D.C. 20554

David Ward
Network Services Division
Common Carrier Bureau
2000 M Street, N.W. - Room 210N
Washington, D.C. 20554

Lawrence Petak
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20554

Charles Isman
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20554

Jim Burtle
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20554

David Sylvar
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20554

The Honorable Janet Reno
Attorney General
Department of Justice
Constitution Ave. & 10th Street, N.W.
Washington, D.C. 20530

The Honorable Steve Colgate
Assistant Attorney General
Department of Justice
Constitution Ave. & 10th Street, N.W.
Washington, D.C. 20530

Stephen W. Preston
Deputy Assistant Attorney General
Civil Division
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530

The Honorable Louis J. Freeh
Director
Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

H. Michael Warren, Section Chief
CALEA Implementation Section
Federal Bureau of Investigation
14800 Conference Center Drive, Suite 300
Chantilly, Va. 22021

James X. Dempsey
Daniel J. Weitzner
Center for Democracy and Technology
1634 Eye Street, N.W. Suite 1100
Washington, D.C. 20006

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas Meeds LLP
1735 New York Avenue, N.W.
Suite 500
Washington, D.C. 20006

Thomas Wheeler
Michael Altschul
Randall S. Coleman
Cellular Telecommunications Industry Assoc.
1250 Connecticut Ave., N.W., Suite 200
Washington, D.C. 20036

Jay Kitchen
Mark J. Golden
Robert Hoggarth
Personal Communications Industry Assoc.
500 Montgomery Street, Suite 700
Alexandria, Va. 22314

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Roy Neel
Linda Kent
Keith Townsend
Lawrence Sarjeant
United States Telephone Association
1401 H Street, N.W., Suite 600
Washington, D.C. 20005

Carole C. Harris
Christine M. Gill
Anne L. Fruehauf
McDermott, Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
AT&T Corporation
Room 3252F3
295 North Maple Avenue
Basking Ridge, New Jersey 07920

Douglas I. Brandon
AT&T Wireless Services
Fourth Floor
1150 Connecticut Avenue
Washington, D.C. 20036

David N. Lace
B. Lynn F. Ratnavale
Lukas, Nace, Gutierrez & Sachs Chartered
1111 19th Street, N.W., Suite 1200
Washington, D.C. 20036

David L. Sobel, Esq.
General Counsel
Electronic Privacy Information Center
666 Pennsylvania Avenue, S.E.
Suite 301
Washington, D.C. 20003

Steven Shapiro, Esq.
Legal Director
American Civil Liberties Union
125 Broad Street
New York, New York 10004

Barry Steinhardt, Esq.
President
Electronic Frontier Foundation
1550 Bryant Street
Suite 725
San Francisco, CA 94103

Kurt A. Wimmer, Esq.
Gerard J. Waldron, Esq.
Alane C. Weixel, Esq.
Covington & Burling
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566

L. Marie Guillory
Jill Canfield
National Telephone Cooperative
Association
2626 Pennsylvania Avenue, N.W.
Washington, D.C. 20037

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Yates
Frank C. Magill
SBC Communications, Inc.
One Bell Plaza, Suite 3703
Dallas, TX 75202

Robert Vitanza
15660 Dallas Parkway
Suite 1300
Dallas, TX 75248

Lisa M. Zaina
Stuart Polikoff
OPASTCO
21 Dupont Circle, N.W.
Suite 700
Washington, D.C. 20036

Elaine Carpenter
Aliant Communications
1440 M Street
Lincoln, NE 68508

John F. Raposa
Richard McKenna
GTE Service Corporation
600 Hidden Ridge, HQE03J36
P.O. Box 152092
Irving, TX 75015-2092

Andre J. Lachance
GTE Service Corporation
1850 M Street, N.W., Suite 1200
Washington, D.C. 20036

Catherine Wang
Swidler & Berlin Chtd.
3000 K Street, N.W.
Suite 300
Washington, D.C. 20007

William T. Lake
John H. Harwood II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

Katherine Marie Krause
Edward M. Chavez
1020 19th Street, N.W.
Washington, D.C. 20036
Stephen G. Kraskin
Sylvia Lesse
Joshua Seidemann
Kraskin, Lesse & Cosson, LLP
2120 L Street, N.W., Suite 520
Washington, D.C. 20037

William L. Roughton, Jr.
PrimeCo Personal Communications, L.P.
601 13th Street, N.W.
Suite 320 South
Washington, D.C. 20005

Barbara J. Kern
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

Joseph R. Assenzo
Sprint Spectrum L.P.
4900 Main Street, 12th Floor
Kansas City, MO 64112

Susan W. Smith
Director, External Affairs
CenturyTel Wireless, Inc.
3505 Summerhill Road
No. 4 Summer Place
Texarkana, TX 75501

Richard J. Metzger
Emily M. Williams
Association for Local
Telecommunications Services
888 17th Street, N.W., Suite 900
Washington, D.C. 20006

Pamela J. Riley
David A. Gross
AirTouch Communications, Inc.
1818 N Street, N.W.
Suite 320 South
Washington, D.C. 20036

Michael W. Mowery
AirTouch Communications, Inc.
2999 Oak Road, MS1025
Walnut Creek, CA 95596

Peter M. Connolly
Koteen & Naftalin
1150 Connecticut Avenue, N.W.
Washington, D.C. 20036

Stephen L. Goodman
William F. Maher, Jr.
Halprin, Temple, Goodman & Sugrue
1100 New York Avenue, N.W.
Suite 650, East Tower
Washington, D.C. 20005

Emilio W. Cividanes
Piper & Marbury, L.L.P.
1200 19th Street, N.W.
Washington, D.C. 20036

M. Robert Sutherland
Theodore R. Kingsley
BellSouth Corporation
1155 Peachtree Street, N.E.
Suite 1700
Atlanta, GA 30309-3610

Michael P. Goggin
BellSouth Cellular Corp.
1100 Peachtree Street, N.E.
Suite 910
Atlanta, GA 30309-4599

J. Lloyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Charles M. Nalbhone
BellSouth Personal Communications, Inc.
3353 Peachtree Road, N.E.
Suite 400
Atlanta, GA 30326

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbrige Center Drive
4th Floor
Woodbridge, NJ 07095-1106

Jill F. Dorsey
General Counsel/Vice President
Powertel, Inc.
1233 O.G. Skinner Drive
West Point, GA 31833

Glenn S. Rabin
Federal Regulatory Counsel
AllTel Communications, Inc.
655 15th Street, N.W., Suite 220
Washington, D.C. 20005

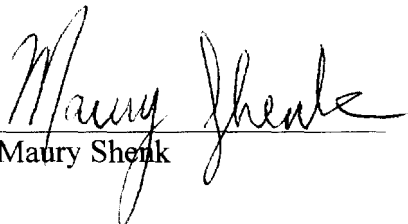
Robert S. Foosaner
Lawrence R. Krevor
Laura L. Holloway
Nextel Communications, Inc.
1450 G Street, N.W.
Suite 425
Washington, D.C. 20005

Judith St. Ledger-Roty
Paul G. Madison
Kelley Drye & Warren, LLP
1200 19th Street, N.W., Suite 500
Washington, D.C. 20036

Kevin C. Gallagher
Senior Vice President
360° Communications Company
8725 W. Higgins Road
Chicago, IL 60631

John T. Scott, III
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

James F. Ireland
Theresa A. Zeterberg
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006


Maury Shenk

DRAFT

*** FOR OFFICIAL USE ONLY ***

February 12, 1997

The intent of this paper is to describe functional capabilities in order to determine costs associated with each of the capabilities. Detailed technical specifications will be provided for the following functional capabilities at a later time. The capabilities are not listed in any order of importance. This list is based on Revision 12 of PN-3580.

Core Evidentiary/ "Minimization":

Subject-Initiated Multiparty Calls

The ability to monitor a multiparty call involving two or more associates, when the intercept subject disconnects from the conference call, but the subject's service continues to support the communications of the associates.

Party Hold Message

The Party Hold message reports the placing of one or more parties of a call on hold by the intercept subject. The Party Hold message is triggered when one or more associates in an active call are placed on hold (e.g., call hold, call waiting, three-way calling, conference calling).

Party Join Message

The Party Join message reports the addition of a call party to an active call or the retrieval of a held call by the intercept subject. The Party Join message is triggered when:

- One or more previously held associates are added to the current call (e.g., call waiting, three-way calling, conference calling)
- An associate joins an existing call with an intercept subject (e.g., barge-in).

Party Drop Message

The Party Drop message reports when a party to a call is released, and the call continues with two or more other parties. The Party Drop message is triggered when a party is released from a multi-way call (e.g., three-way calling, conference call, meet-me conference). (Note: Release of an entire call is reported by the Release message, not the Party Drop message.)

Call Control (Subject Input) Message

The Call Control message reports intercept subject inputs detected by a control function. A control function is any function within a switching or service control system that collects and interprets user inputs to provide features or services. The inputs reported include digits dialed and any special keys used. Inputs may be accumulated and sent

*** FOR OFFICIAL USE ONLY ***

DRAFT

DRAFT

*** FOR OFFICIAL USE ONLY ***

February 12, 1997

when the system can perform some action or when an event precludes acting upon the input, such as call abandonment or partial dial time-out. The Call Control message is triggered when:

- A feature key is detected.

~~• A string of digits is detected, which may or may not be interpreted (e.g., an unrouteable number)~~

~~• A string of digits is detected with an input to abandon the attempt (i.e., subject goes on-hook)~~

~~• A string of digits is detected, but an input timer expires~~

[ABOVE SCENARIOS ARE COVERED BY THE ORIGINATION MESSAGE]

- A switchhook flash or its equivalent is detected.

Notification Message (Call Progress Tones and Voice Message Waiting Indication)

The Notification message reports out-of-band signaling sent that can be sensed by the intercept subject or an associate. The Notification message is also used to report in-band signaling applied by the accessing system. The Notification message is triggered when:

- The accessing system applies an in-band audible indication to the intercept subject's receive content channel, such as:
 - Call progress tones (e.g., dial, recall, busy, or reorder tones)
 - Any alerting of incoming calls or messages (e.g., call waiting tone or message waiting tone).
- The accessing system sends or passes a command to the intercept subject's terminal to activate or deactivate:
 - Audible indications (e.g., annunciator to indicate call waiting or alerting: power alert/ringing, distinctive alert/ringing, recall alert/dial tone, or call forwarding reminder alert/ring, busy tone, or reorder tone)
 - Visual indications (e.g., lights to indicate call waiting)
 - Alphanumeric display information (e.g., messages permanently stored in the terminal or messages sent by the switch: calling number identification, calling name identification, or display information).
- The accessing system applies an in-band audible indication to the associate's receive channel for incoming call attempts to a subject, such as:

*** FOR OFFICIAL USE ONLY ***

DRAFT

DRAFT

*** FOR OFFICIAL USE ONLY ***

February 12, 1997

- Call progress tones
- Any alerting of incoming calls or messages.
- The accessing system sends or passes a command to the associate's terminal, in support of communications with the intercept subject, to control the generation of:
 - Audible indications
 - Visual indications
 - Alphanumeric display information.

Timing

The timestamp on each of the call event messages is accurate within 100 milliseconds of the events and is delivered from the intercept access point to the demarcation point at the carrier facility within 500 milliseconds.

*** FOR OFFICIAL USE ONLY ***

DRAFT

DRAFT

*** FOR OFFICIAL USE ONLY ***

February 12, 1997

Integrity of Interception Efforts:**Surveillance Status Message**

The Surveillance Status message reports the status of a surveillance for particular subject whenever a surveillance is activated, updated, or deactivated. The message is also sent periodically from once every hour to once every 24 hours for the duration of a surveillance. The activate and update status messages will report the call content channels assigned to the surveillance. The Surveillance Status message is triggered when:

- The surveillance is activated, updated, or deactivated
- Periodically for the duration of the surveillance.

Continuity Check for Dedicated CCCs

A continuous signal or tone (DTMF C-tone) should be applied on all dedicated, nailed-up CCCs as a continuity check.

Manageability of Effecting Interception:**X.25 Data Transfer Service for Call Data Channel (CDC)**

The ability to provide call-identifying messages within X.25 packets at the demarcation point. X.25 and related protocols should be supported over both analog and digital DS1 wireline interfaces. The demarcation point is the carrier's end of the circuit procured by the law enforcement agency for delivery to that agency's monitoring site.

CCC Protocols

The ability to provide call content channels at the demarcation point over either an analog wireline circuit or digital DS1 wireline circuit.

Feature Status Message

The Feature Status message reports the assignment, removal, activation, or deactivation of network-provided features, by an intercept subject or the service provider, that would impact the delivery to law enforcement of call content and/or call-identifying information related to that subject. The Feature Status message is triggered when:

- ~~The equipment, facilities, or services of an intercept subject are used to activate or deactivate a feature that would impact the delivery to law enforcement of call content and/or call-identifying information~~

[THIS SCENARIO IS COVERED BY THE ORIGINATION MESSAGE]

*** FOR OFFICIAL USE ONLY ***

DRAFT